Aj	Authenticator of Terminal **J**	**L**	License, Certificate
Ao	Certificate Module	**Li**	License, Certificate issued to **I**
Bi	Token of User **I**	**LE**	Certificate of key **E**
Co	System Master Common Key	**LV**	Certificate of key **V**
Ci	Common Key of User **I**, symmetric key	**M**	Plaintext
Di	Private Decryption Key of User **I**, asymmetric key	**Mi**	Plaintext to or from User **I**
		Ni	ID# of User **I**
Ei	Public Encryption Key of User **I**	**NR**	Random Number
F	Unique Feature	**O**	System Authority
Fi	Unique Feature of User **I**	**P**	Ciphertext
F1	First Unique Feature (PIN/Password)	**Pi**	Ciphertext of User **I**
F2	Second Unique Feature (Biometrics)	**Qi**	Challenge Message sent to User **I**
G	Value of Mode Counter	**Ri**	Response Message from User **I**
G1	Value of Mode 1 Counter	**Si**	Signing Key of **I**
G2	Value of Mode 2 Counter	**So**	Signing Key of **O**
G3	Value of Mode 3 Counter	**TC**	Expiration Date of **Ci**
G4	Value of Mode 4 Counter	**TE**	Expiration Date of Certificate **LE**
H	Authentication Reference Hash Value of Unique Feature	**TL**	Logon Time
H1	Hash Value of PIN or Password **F1**	**TM**	Mode Expiration Period
H2	Feature Vector of Biometrics **F2**	**TP**	Present Time
I	User	**TV**	Expiration Date of Certificate **LV**
J	Local Terminal	**Ui**	Message Authorized by **I**, signed by **Si**
K	Key **C, D, E, S, V**	**Vi**	Verification key of **I**
K {M}	Cryptographic Operation M is encrypted by **K**	**Vo**	Verification key of **O**

FIG 1: Notation

(201) $P = K \{M\}$ M is encrypted by K

(202) $M = K \{P\}$ P is decrypted by K

(203) $TP - TL \leq TM$

(204) $G > 0$

(205) $Ci = Co \{Ni + TC\}$

(207) $LEi = So \{Ni, Ei, TE\}$

(208) $Vo \{LEi\} => Ni, Ei, TE$

(209) $LVi = So \{Ni, Vi, TV\}$

(210) $Vo \{LVi\} => Ni, Vi, TV$

(211) $Qi = NR + TP$

(212) or $Qi = Mi + TP$

(213) $Ri = Ci \{Qi\}$

(214) $Ci \{Ri\} => Qi$
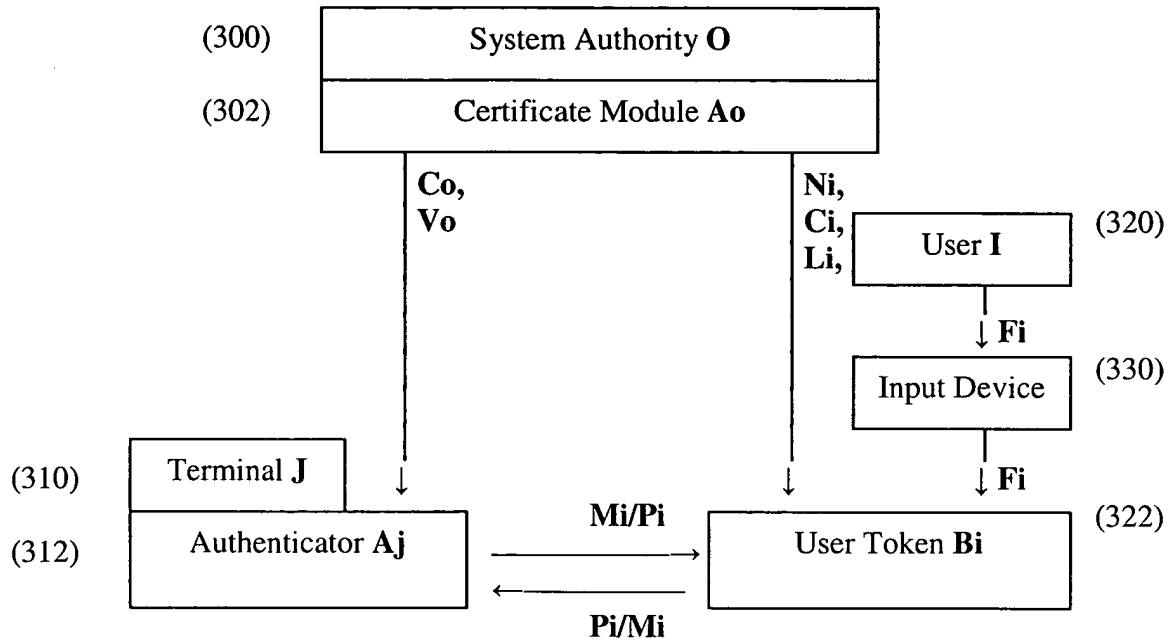
(215) $Ri = Di \{Qi\}$

(216) $Ei \{Ri\} => Qi$

(217) $Pi = Ei \{Mi\}$

(218) $Mi = Di \{Pi\}$

(219) $Ui = Si \{Mi\}$

(220) $Vi \{Ui\} => Mi$

FIG 2: Formulae

(300) System Authority **O**

(302) Certificate Module **Ao**

Co,
Vo

Ni,
Ci,
Li,

User **I** (320)

↓ **Fi**

Input Device (330)

(310) Terminal **J**

(312) Authenticator **Aj**

Mi/Pi →

↓ **Fi**

User Token **Bi** (322)

← **Pi/Mi**

Ci	Common Key of User **I**, symmetric key
Co	System Master Common Key
Fi	Unique Feature of User **I**
Li	License, Certificate issued to User **I**
Mi	Plaintext to or from User **I**
Ni	ID# of User **I**
Pi	Ciphertext of User **I**
Vo	Verification key of **O**

FIG 3: Block Diagram of the System of This Invention

Mode	Logon Expiration Period TM	Application Security Level
0	No Limit	No Security
1	1 week	Low
2	1 day	Middle
3	1 sign	High
4	1 sign	Highest

FIG 4: An Example of the Modes of a Multi-Mode Token

Register Name	Value in Register
Logon Time Register	**TL**
Mode 1 Counter	**G1**
Mode 1 Expiration Period	**TM1**
Mode 2 Counter	**G2**
Mode 2 Expiration Period	**TM2**
Mode 3 Counter	**G3**
Mode 4 Counter	**G4**

FIG 5: The Register & Counter values of a Multi-Mode Token

Item	Notation & Data	Secret
User Name		
Token ID #	Ni	
Common Key	C	X
Expiration Date of C	TC	
Private Decryption Key	D	X
Public Encryption Key	E	
Certificate of Ei	LE	
Expiration Date of LE	TE	
Private Signing Key	S	X
Public Verification Key	V	
Certificate of V	LV	
Expiration Date of LV	TV	
Public Verification Key of O	Vo	
Authentication Reference		
Hash Value of PIN or Password	H1	X
Feature Vector of Biometrics	H2	X

FIG 6: A Table of the Basic User Data Stored in a Multi-Mode Token

Mode	Crypt Key	Crypt Operand bit	Usage Condition			Application			
			Logon	Access Times G max	Expiration Period TM	Decrypt	Sign for		
							Authentication	Payment	Authorization
0	N/A	N/A	Free						
1	C	No Limit	F1 or F2	10	1 week		Low		
2	D	< 1024	F1 or F2	5	1 day	Session Key, File Key	High	Micro	
3	S	≤ 64	F1 or F2	1	1 session			Regular	Regular
4	S	> 64	F1 and F2	1	1 session			Large	Important

FIG 7: An Example of Multi-Mode Settings

Certificate Module **Ao**	User Token **Bi**

(800) Generate **Co, So, Vo**

(801) Get User Name, ID # **Ni** & Initial **Ci, H1i, H2i**

(804) Setup Session

(806) Request New **Ci**, Send **Ni**

←

(807) Derive New **Ci** $Ci = Co \{Ni + TC\}$

(808) Return **Ci, TC**

→

(809) Store New **Ci, TC**

Ci   Common Key of User **I**, symmetric key

Co   System Master Common Key

H1i   Hash Value of PIN or Password

H2i   Feature Vector of Biometrics

So   Signing Key of **O**

TC   Expiration Date of **Ci**

Vo   Verification Key of **O**

{ }   Cryptographic Operation

FIG 8A: Initialization Flow of Token

Certificate Module **Ao**	User Token **Bi**

(816) Request **Di, Ei, LEi** Send **Ni**

(817) Generate **Di, Ei, LEi**
LEi = So {Ni, Ei, TE}

(818) Return **Di, Ei, LEi, TE**

(819) Store **Di, Ei, LEi, TE**

(823) Generate **Si, Vi**

(826) Request **LV**, Send **Ni, Vi**

(827) Generate **LVi**
LVi = So {Ni, Vi, TV}

(828) Return **LVi, TV**

(829) Store **Si, Vi, LVi, TV**

FIG 8B: Initialization Flow of a Token (continued)

Authentication Module **Aj**	User Token **Bi**	User **I**

(902) — Operation require Log on (**F1/F2**) ← Original Flow (xxx)

(904) — Set up Session

(906) — Request Display "Log on (**F1/F2**)"

(907) — Display "Log on (**F1/F2**)"

(910) — Input **F1i/F2i**

(911) — Verify **F1/F2** by **H1/H2**

(912) — Request Date

(914) — Return Present Date **TP**

(915) — Reset
TL = TP
G1 = G1 max = 10
G2 = G2 max = 5
G3 = G3 max = 1
G4 = G4 max = 1
→ Original Flow (xxx)

FIG 9: Flow of Multi-Mode Token Logon

Authentication Module **Aj**	User Token **Bi**

(1003)　　　　　　　　　　　　　　Status needs to be Authenticated

(1004)　　　　　　　　　　Set up Session

(1006)　　　　　　Req. Authentication, Send **Ni**

　　　　　　　　　　　　　　←

(1007)　　Generate **Qi**
　　　　　Qi = NR + TP

(1008)　　　　　　Req. Sign by C, Send **Qi**

　　　　　　　　　　　　　　→

(1011)　　　　　　　　　　Check **TP**
　　　　　　　　　　　TP – TL ≤ TM1

(1012)　　　　　　　　　　Check **G1 > 0**

(1014)　　　　　　　　　Calculate Response
　　　　　　　　　　　Ri = Ci {Qi}

(1015)　　　　　　　　　**G1 = G1 - 1**

(1016)　　　　　　Respond **Ri, TC**

　　　　　　　　　　　　　　←

(1017)　　Verify **TC, Ri**
　　　Ci = Co {Ni + TC}
　　　　Ci {Ri} => Qi

(1018)　　　　　　Send Result

　　　　　　　　　　　　　　→

FIG 10: Flow of Mode 1 Operation

Authentication Module **Aj**	User Token **Bi**

(1103) | | Status needs to be Authenticated |

(1104) | Set up Session |

(1106) | Req. Authentication, Send **Ni** |

←

(1107) | Generate **Qi** $Qi = NR + TP$ |

(1108) | Req. Sign by **D**, Send **Qi** |

→

(1111) | Check **TP** $TP - TL \leq TM2$ |

(1112) | Check $G2 > 0$ |

(1114) | Calculate Response $Ri = Di \{Qi\}$ |

(1115) | $G2 = G2 - 1$ |

(1116) | Return **Ri, LEi** |

←

(1117) | Verify **LEi, Ri** $Vo \{LEi\} \Rightarrow Ni, Ei, T1$ $Ei \{Ri\} \Rightarrow Qi$ |

(1118) | Send Result |

→

FIG 11: Flow of Mode 2, Authentication

Authentication Module **Aj**	User Token **Bi**

(1202) | Has Cipher Message **Pi** |

(1204) | Set up Session |

(1208) | Req. Decryption, Send **Pi** & **TP** |

(1211) | Check **TP** $$TP - TL < TM2$$ |

(1212) | Check **G2 > 0** |

(1214) | Decrypt **Pi** $$Mi = Di \{Pi\}$$ |

(1215) | **G2 = G2 - 1** |

(1216) | Return **Mi** |

FIG 12: Flow of Mode 2, Decryption

	Authentication Module **Aj**	User Token **Bi**
(1302)	Has Payment Message **Mi**	
(1304)	Set up Session	
(1307)	**Qi = Mi + TP**	
(1308)	Req. Sign by **D**, Send **Qi**	
(1311)		Check **TP** **TP – TL < TM2**
(1312)		Check **G2 > 0**
(1314)		Sign on **Qi** **Ri = Di {Qi}**
(1315)		**G2 = G2 - 1**
(1316)	Return **Ri, LEi**	
(1317)	Verify **LEi, Ri** Vo {LEi} => Ni, E1i, T1 Ei {Ri} => Qi	
(1318)	Send Result	

FIG 13: Flow of Mode 2, Payment

(1402) Authentication Module **Aj**

Has **Mi** to be signed

User Token **Bi**

(1404) Set up Session

(1408) Req. Sign by **S**, Send **Mi**

(1409) Check **Mi** ≤ 64 bit

(1410) Require Logon **F1** or **F2**   → (902)
                                         ← (915)

(1412) Check
G3 > 0

(1414) Sign on **Mi**
Ui = Si {Mi}

(1415) **G3 = G3 - 1**

(1416) Return **Ui, LVi**

(1417) Verify **LVi, Ui**
Vo {LVi} => Ni, Vi, TV
Vi {Ui} => Mi

(1418) Send Result

FIG 14: Flow of Mode 3 Payment/Authorization

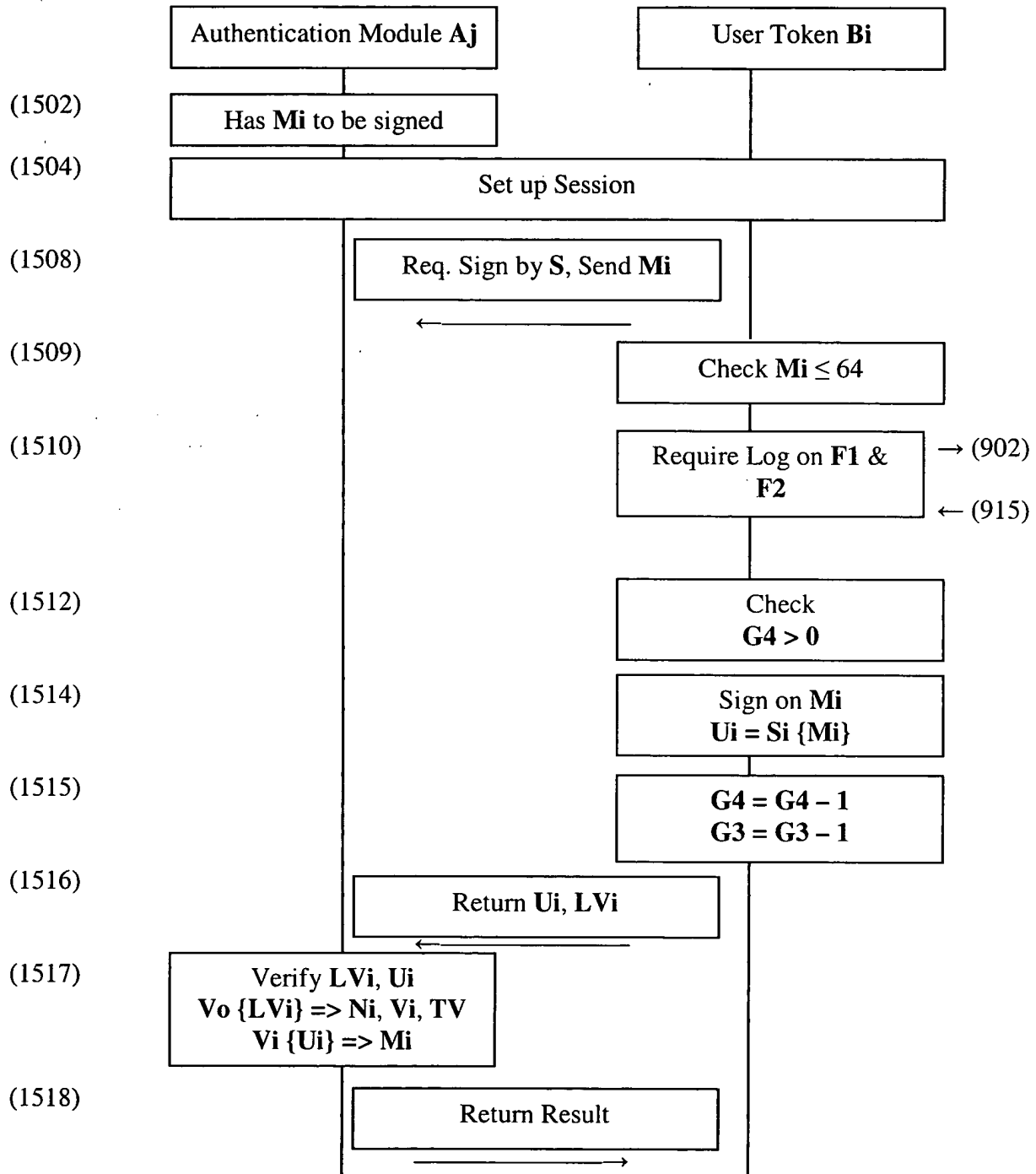|		
	Authentication Module **Aj**	User Token **Bi**
(1502)	Has **Mi** to be signed	
(1504)	Set up Session	
(1508)	Req. Sign by **S**, Send **Mi**	
(1509)		Check **Mi** ≤ 64
(1510)		Require Log on **F1** & **F2** → (902) ← (915)
(1512)		Check **G4 > 0**
(1514)		Sign on **Mi** **Ui = Si {Mi}**
(1515)		**G4 = G4 − 1** **G3 = G3 − 1**
(1516)	Return **Ui, LVi**	
(1517)	Verify **LVi, Ui** **Vo {LVi} => Ni, Vi, TV** **Vi {Ui} => Mi**	
(1518)	Return Result	

FIG 15: Flow of Mode 4 Payment/Authorization